

What is Claimed is:

1. An encryption system comprising:

a transmitting device for modulating data with a pseudo-random signal for signalling over a transmission medium; and

5 a receiving device for receiving said data by removing said pseudo-random signal.

2. The system of claim 1 wherein said transmitting device further comprises:

means to generate a second modulated signal;

10 means to add said second modulated signal to said data signal to produce a transmitted signal; and

means to send said transmitted signal over a transmission medium.

3. The system of claim 2 wherein said receiving device further comprises:

means to generate a third modulated signal;

15 means to subtract said third modulated signal from said transmitted signal to produce a data output signal; and

means to demodulate said output signal to produce a second data output signal.

4. The system of claim 3 wherein said second modulated signal and said third modulated signal are pseudo-random and opposite in amplitude, but otherwise identical in phase and frequency, thereby simplifying the demodulation of said data.

20

5. The system of claim 4 wherein the parameters defining the phase, amplitude and frequency of said second modulated signal and said third modulated signal are derived from a random number generator seeded with a key, thereby increasing the difficulty of an intruder planning to intercept said transmitted signal.

6. The system of claim 5 wherein said random number generator is implemented at both the transmitter and receiver and seeded with the same key so that parameters derived from both are the same and when applied to said means for generating said second modulated signal and said means for generating said third modulated signal result in the same signal being generated, thereby ensuring correct reception of said transmitted signal.
7. The system of claim 6 wherein the data is manipulated as a 'group of bits' and the number of bits in a 'group of bits' is a parameter and may be varied for each 'group of bits'.
- 10 8. The system of claim 7 wherein said number of bits parameter is derived from a second random number generator.
9. The system of claim 7 wherein said number of bits parameter is derived from the same random number generator as used for the parameters defining said second modulated signal and said third modulated signal.
- 15 10. A method of encrypting data comprising the steps of:
- modulating data with a pseudo-random signal for signalling over a transmission medium;
- transmitting said data;
- receiving said data; and
- 20 removing said pseudo-random signal.